FORTINET

Release Notes

FortiSwitchOS 7.2.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

October 10, 2022
FortiSwitchOS 7.2.2 Release Notes
11-722-830761-20221010

TABLE OF CONTENTS

Change log

Date	Change Description
September 2, 2022	Initial release for FortiSwitchOS 7.2.2
October 10, 2022	Updated the “Product integration and support” section.

Introduction

This document provides the following information for FortiSwitchOS 7.2.2 build 0419.

See the Fortinet Document Library for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.2.2 supports the following models:

FortiSwitch 1xx	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE
FortiSwitch 2xx	FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE
FortiSwitch 4xx	FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448E, FS-448E-POE, FS-448E-FPOE
FortiSwitch 5xx	FS-524D, FS-524D-FPOE, FS-548D, FS-548D-FPOE
FortiSwitch 1xxx	FS-1024D, FS-1024E, FS-1048E, FS-T1024E
FortiSwitch 3xxx	FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What's new in FortiSwitchOS 7.2.2

Release 7.2.2 provides the following new features:

- You can now specify static entries for DHCP snooping and DAI by manually associating an IP address with a MAC address in the CLI.
- You can now override the global option-82 setting for DHCP requests by specifying plain text strings for the Circuit ID field and the Remote ID field for a specific VLAN on a port.
- You can now use the GUI to configure MLD snooping on FortiSwitch VLANs.
- You can now use the following wildcard characters in the `set value` command for the automation trigger used for an automation stitch:
  - Use an asterisk to match any character string of any length, including 0-characters long. For example, use `set value "*1567*"` to match values of `81567` and `156789`.
  - Use square brackets to match one of the multiple characters. For example, use `set value "[aA]dmin"` to match values of `admin` and `Admin`.
- You can now configure multiple fields for the automation trigger used for an automation stitch when the `event-type` is `event-log` and the `logid` is set. The action is only performed if all conditions are valid (using AND logic).
- You can use a new CLI command to change how a FortiSwitch unit with Power over Ethernet (PoE) disconnects from a powered device:

```
config switch physical-port
   edit <port_name>
      set poe-disconnection-type {AC | DC | DC-delay}
   next
end
```

- VXLAN tunnels are now supported on FS-3032E.
- If an unverified firmware image is uploaded to FortiSwitchOS, the following warning is displayed in the GUI: "WARNING: This firmware failed signature validation."
- You can now display IPv4 and IPv6 routes by VRF instance on the *Router* > *Monitor* > *Routing* and *Router* > *Monitor* > *IPv6 Routing* pages.
- The default value for the `set dhcp-snoop-client-req` command (under `config system global`) is now `drop-untrusted`, instead of `forward-untrusted`.
- The new `set ebgp-requires-policy` command (under `config router bgp`) is set to `enable` by default, which prevents the BGP router from learning or advertising prefixes from or to its eBGP peers.
- Under the `config router ospf` command, `set ucast-ttl` has been renamed to `set ttl`. This setting now applies to multicast OSPF packets, as well as unicast OSPF packets.

Refer to the FortiSwitch feature matrix for details about the features supported by each FortiSwitch model.

Special notices

Zero-touch management

When a new FortiSwitch unit is started, by default, it will connect to the available manager, which can be a FortiGate device, FortiLAN Cloud, or FortiSwitch Manager. All ports are enabled for auto discovery. The “internal” interface is the DHCP client in all FortiSwitch models. If you do not want your FortiSwitch unit to be managed, you must disable the features that you do not want active.

By default, auto-network is enabled in FortiSwitchOS 7.2.0 and later

After an `execute factoryreset` command is executed on a FortiSwitch unit in standalone mode, the auto-network configuration is enabled by default. If you are not using auto-network, you must manually disable it:

```
config switch auto-network
   set status disable
end
```

Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported

Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.2.6 and later 6.2 versions is supported. Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.4.4 and later 6.4 versions is supported. Downgrading FortiSwitchOS 7.0.0 to versions earlier than FortiSwitchOS 6.2.6 or 6.4.4 is not supported.

Downgrading FortiSwitchOS 7.0.0 and later requires converting the admin password first

Because FortiSwitchOS 7.0.0 changed from SHA1 to SHA256 encryption for admin passwords, you need to convert the format of the admin password before downgrading from FortiSwitchOS 7.0.0 and later to an earlier FortiSwitchOS version.

If you do not convert the admin password before downgrading from FortiSwitchOS 7.0.0 and later, the admin password will not work after the switch reboots with the earlier FortiSwitchOS version.

The encrypted admin password in FortiSwitchOS 7.0.0 and higher starts with “SH2”, and the encrypted admin password for earlier FortiSwitchOS versions starts with “AK1”.

To convert the format of the admin password in FortiSwitchOS 7.0.0 and later before downgrading to an earlier FortiSwitchOS version:

1. Enter the following CLI command to convert the admin password from SHA256 to SHA1 encryption:

   ```
   execute system admin account-convert <admin_name>
   ```

2. Downgrade your firmware.

Connecting multiple FSR-112D-POE switches

The FSR-112D-POE switch does not support interconnectivity to other FSR-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

Upgrade information

FortiSwitchOS 7.2.2 supports upgrading from FortiSwitchOS 3.5.0 and later.

For FortiSwitch units managed by FortiGate units, refer to the *FortiLink Release Notes* for upgrade information.

Product integration and support

FortiSwitchOS 7.2.2 support

The following table lists FortiSwitchOS 7.2.2 product integration and support information.

Web browser	• Mozilla Firefox version 52 • Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS (FortiLink Support)	Refer to the FortiLink Compatibility table to find which FortiSwitchOS versions support which FortiOS versions.

Resolved issues

The following issues have been fixed in FortiSwitchOS 7.2.2. For inquiries about a particular bug, please contact Customer Service & Support.

718440	When 802.1X MAC-based authentication, dynamic VLAN assignment, and allow-mac-move are configured, the FortiSwitch unit incorrectly forwards packets with VLAN tags.
795041	The VM debug report (*System* > *Debug Report*) is missing information for many CLI commands.
814741	MAC authentication bypass (MAB) authentication sometimes does not work on a managed FS-108E.
818959	The DHCP server does not allow DHCP clients to move from one interface to another.
821808	After using the FortiSwitch Configuration Migration Tool, all VLANS are missing.
824283	The output of the `diagnose switch physical-ports qos-stat list` command shows the same number of dropped packets for queue 0 for all ports.
825614	The status of the second power supply unit is incorrectly reported as “Not OK.”
830533	After upgrading to FortiSwitchOS 7.2.1, the status of the single power supply unit is incorrectly reported as “Not OK,” and the status of the fan is incorrectly reported as more than 100 percent.
831495	The TV multicast receivers do not unsubscribe from the multicast stream.
831546	Logging in to a FortiSwitch unit that is managed by FortiSwitch Manager displays a message that incorrectly refers to FortiLink and FortiGate.

Common vulnerabilities and exposures

FortiSwitchOS 7.2.2 is no longer vulnerable to the following vulnerabilities and exposures:

- CVE-2022-31116
- CVE-2022-31117

Visit https://fortiguard.com/psirt for more information.

Known issues

The following known issues have been identified with FortiSwitchOS 7.2.2. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
382518, 417024, 417073, 417099, 438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANs).
414972	IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality.
480605	When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server. **Workarounds:** —Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN. —Temporarily disable dhcp-snooping on vlan, issue the `execute interface dhcpclient-renew <interface>` command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.
510943	The time-domain reflectometer (TDR) function (cable diagnostics feature) reports unexpected values. **Workaround:** When using the cable diagnostics feature on a port (with the `diagnose switch physical-ports cable-diag <physical port name>` CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.
542031	For the 5xx switches, the `diagnose switch physical-ports led-flash` command flashes only the SFP port LEDs, instead of all the port LEDs.
548783	Some models support setting the mirror destination to “internal.” This is intended only for debugging purposes and might prevent critical protocols from operating on ports being used as mirror sources.
572052	Backup files from FortiSwitchOS 3.x that have 16-character-long passwords fail when restored on FortiSwitchOS 6.x. In FortiSwitchOS 6.x, file backups fail with passwords longer than 15 characters. **Workaround:** Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x.
585550	When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded.

Bug ID	Description
606044/610149	The results are inaccurate when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
609375	The FortiSwitchOS supports four priority levels (critical, high, medium, and low); however, The SNMP Power Ethernet MIB only supports three levels. To support the MIB, a power priority of medium is returned as low for the PoE MIB.
659487	The FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE, FS-148E, and FS-148E-POE models support ACL packet counters but not byte counters. The `get switch acl counters` commands always show the number of bytes as 0.
667079	For the FSR-112D-POE model: • If you have enabled IGMP snooping or MLD snooping, the FortiSwitch unit does not support IPv6 functionalities and cannot pass IPv6 protocol packets transparently. • If you want to use IGMP snooping or MLD snooping with IPv6 functionalities, you need to enable `set flood-unknown-multicast` under the `config switch global` command.
673433	Some 7-meter DAC cables cause traffic loss for the FS- 448E model.
748210	The MAC authentication bypass (MAB) sometimes does not work on the FS-424E when a third-party hub is disconnected and then reconnected.
784585	When a dynamic LACP trunk has formed between switches in an MRP ring, the MRP ring cannot be closed. Deleting the dynamic LACP trunk does not fix this issue. MRP supports only physical ports and static trunks; MRP does not support dynamic LACP trunks. **Workaround:** Disable MRP and then re-enable MRP.
793145	VXLAN does not work with the following: • log-mac-event • DHCP snooping • LLDP-assigned VLANs • NAC
829807	eBGP does not advertise routes to its peer by default unless the `set ebgp-requires-policy disable` command is explicitly configured or inbound/outbound policies are configured.

www.fortinet.com